APROB
Rectorul USEFS,
dr. hab., prof. univ.
V.Manolachi
„15” ianuarie 2015

REGULAMENTUL PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ CONTABILĂ

I. DISPOZIŢII GENERALE

1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă (în continuare Regulament) este elaborat în vederea implementării în cadrul USEFS-a prevederilor Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal, Legii contabilităţii nr. 113 din 27 aprilie 2007 şi a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14 decembrie 2010, precum şi întru respectarea prevederilor art. 91 - 94 ale Codului muncii al Republicii Moldova.

1.2. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale angajaților USEFS în cadrul sistemului de evidență contabilă.

II. SCOPUL

2.1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă constă în asigurarea înregistrării informațiilor contabile referitoare la calculul drepturilor salariale ale angajaților, inclusiv a premiilor, stimulărilor, sporurilor, indemnizațiilor, compensațiilor și altor drepturi și obligații cu conținut pecuniar, precum și a prezentării rapoartelor financiare, trimestriale şi anuale către instituţiile statului, conform legislației în vigoare.

2.2. În cadrul sistemului de evidență contabilă sînt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele și patronimicul;
- numărul personal de identificare de stat (IDNP);
- data naşterii şi domiciliul;
- codul personal de asigurări sociale (CPAS);
- datele privind locul de muncă și funcția ocupată;
- mărimea salariului brut și alte premii, sporuri, stimulări, suplimente;
- datele privind situația familială (la cererea solicitantului);
- numele, prenumele (după caz, patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude și persoane, după caz);
- datele pentru transferul pe contul bancar a plăților salariale,burselor și a altor sume datorate cu titlu de indemnizații, compensații sau alte beneficii, după caz;
- datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizației corespunzătoare;

- mărimea concretă a drepturilor salariale calculate, taxele și impozitele aferente, inclusiv contribuțiile de asigurări sociale obligatorii de asistență medicală și socială, și alte sume datorate în virtutea legii sau contractului;
- după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.

1.1. Prelucrarea datelor cu caracter personal menționate va fi efectuată pentru realizarea următoarelor scopuri:

a) Prelucrarea informaţiei privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajaţii şi care au inpact asupra calculării plaţilor salariale, de exemplu: modificarea gradului ştiinţific al cadrelor didactice, sporurile pentru titlurile onorifice, sporurile si suplimente de plată cu caracter stimulator şi de compensare, vechimea in muncă.

b) Calcularea salariilor lunare, în conformitate cu legislaţia în vigoare a Republicii Moldova (Hotărîrea Guvernului nr.195 din 13.03.2013 privind condiţiile de salarizare a personalului în instituţiile de învăţămînt superior de stat cu autonomie financiară, Hotărîrea Guvernului nr.381 din 13.04.2006 cu privire la condiţiile de salarizare a personalului din unitaţile bugetare, Legea nr.355-XVI din 23 decembrie 2005 cu privire la sistemul de salarizare în sectorul bugetar.

c) Prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii indemnizațiilor corespunzătoare;

d) Prelucrarea copiilor ordinelor Rectorului referitoare la personal;

e) Calcularea și reținerea taxelor ce ţin de plăţile salariale aferente angajaților: primele de asigurare obligatorie de asistență medicală, contribuțiile la bugetul asigurărilor sociale de stat, impozitul pe venit, etc.;

f) Calcularea și virarea primelor de asigurare obligatorie de asistență medicală și a contribuțiilor la bugetul asigurărilor sociale de stat, aferente plăților salariale - obligație a angajatorului;

g) Furnizarea informaţiei necesare pentru elaborarea rapoartelor trimestriale privind contribuţiile de asigurare socială de stat obligatorii (forma 4BASS) și primele de asigurare obligatorie de asistență medicală (Formularul MED08);

h) Întocmirea, trimestrială, a declaraţiei persoanei asigurate REV 5 pentru fiecare angajat și transmiterea acestora Casei Teritoriale de Asigurări Sociale, filiala Rîşcani în format electronic prin SIA E-REPORTING și, anual, pe suport de hîrtie;

i) Asistarea procesului (prin furnizarea informaţiei necesare) pentru completarea periodică (lunară) a raportului şi dării de seamă privind venitul achitat şi impozitul pe venit reţinut din acesta;

j) Completarea lunară, trimestrială şi anuală a dărilor de seamă cu prezentarea acestora Inspectoratului Fiscal de Stat Rîşcani (privind impozitul pe venit IRV 09, IAL 09, MED 08), precum şi perfectarea şi eliberarea informaţiei privind veniturile calculate şi achitate în folosul persoanei fizice şi impozitul pe venit reţinut din aceste venituri angajaților USEFS;

k) Prelucrarea cererilor și a documentelor confirmative privind acordarea scutirilor la impozitul pe venit reţinut din salariu, în conformitate cu capitolul 4, titlul II din Codul Fiscal;

l) Eliberarea certificatelor de salariu, la cererea angajaților;

m) Completarea și stocarea fișelor personale de evidenţă a veniturilor sub formă de salariu şi alte plăţi efectuate de către patron în folosul angajatului pe fiecare an, precum şi a impozitului pe venit reţinut din aceste plăţi (Anexa nr. 8 la Ordinul IFPS nr.676 din 14.12.2007).

1.2. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către USEFS astfel încît să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sînt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor expres prevăzute de lege acestea pot rămîne la păstrare primind statut de document de arhivă.

1.3. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență contabilă în alte scopuri decît cele menționate mai sus este interzisă.

III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ CONTABILĂ

3.1. Datele cu caracter personal conținute în sistemul de evidență contabilă în cadrul USEFS se prelucrează/stochează:

1. pe suport de hîrtie;
2. în format electronic:

Software – Sistemul de evidență contabilă în sfera bugetară „1C:Contabilitatea p/u Moldova”, versiunea 8.0., care este instalat la computerul central – „Contabil Șef” și cu drept de acces la cele patru computere, computerele aflîndu-se în birourile nr.204,208 din sediul USEFS,str.A.Doga,22 ;

3.2. Mentenanța programului contabil „1C:Contabilitatea 8 pentru Moldova” este efectuată de către compania „Abandant-Program 1C” ÎM SRL, fiind încheiat anual contract de valoare mică privind prestarea serviciilor de deservire între USEFS și compania „Abandant-Program 1C” ÎM SRL, cu următoarele atribuții stabilite companiei prestatoare:

- Efectuarea ajustărilor în program, în baza modificărilor legislației Republicii Moldova;
- Eliminarea erorilor în funcționarea programului;
- Consultarea în rezolvarea dificultăților apărute în utilizarea programului (Linia fierbinte);
- Examinarea solicitărilor parvenite din partea USEFS;
- Examinarea bazei de date a USEFS (la necesitate);
- Vizite la fața locului, la solicitarea USEFS;
- Examinarea și nedivulgarea informației cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

3.3. Prelucrarea informațiilor în sistemul de evidență contabilă pe suport de hîrtie este structurată după criteriul “mape-dosare”, fiind păstrate în dulapuri, care sînt amplasate fizic în birourile nr.204,206 din sediul USEFS,str.A.Doga,22.

IV. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal în sistemul de evidență contabilă se efectuează pe perioada valabilității activității angajaților USEFS (din momentul semnării contractului pînă la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).

4.2. La expirarea termenelor menționate în punctul 4.1., datele din sistemul de evidență contabilă sînt păstrate în formă arhivată, pe perioada stabilită de Nomenclatorul general stabilit.

V. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

5.1. USEFS, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.

5.2. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.

5.3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență contabilă vor respecta procedura de acces la datele cu caracter personal.

5.4. Acordarea dreptului de acces a angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii USEFS. Informațiile furnizate vor fi acordate astfel, încît să nu prejudicieze drepturile terților. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.

5.5. Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu, dacă în informațiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţămîntul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

VI. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENȚĂ CONTABILĂ

6.1. Măsurile generale de administrare a securităţii informaţionale

6.1.1. În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronic care conţin date preluate din sistemul de evidență contabilă, aceştia se păstrează în safeuri care se încuie.

6.1.2. La terminarea sesiunilor de lucru, computerele şi imprimantele se deconectează de la rețeaua electrică.

6.1.3. Operatorul asigură securitatea punctelor de primire şi expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele de copiere.

6.1.4. Accesul fizic la mijloacele de reprezentare a informaţiei preluate din sistemul de evidență contabilă este blocat împotriva vizualizării de către persoane neautorizate.

6.1.5. Mijloacele de prelucrare a informaţiilor preluate din sistemul de evidență contabilă sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

6.1.6. Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din sistemul de evidență contabilă din/în perimetrul de securitate se înregistrează în registru.

6.2. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidență contabilă, se înfăptuiesc ţinînd cont de necesitatea asigurării confidenţialităţii și integrității acestora, prin protecţie în formă manuală, electronică şi externă.

6.3. Cerințe speciale față de marcare:_toate informațiile ieşite din sistemul de evidență contabilă, care conţin date cu caracter personal, sînt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

6.4. Accesul în biroul unde este amplasat sistemul de evidență contabilă este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces și cheia de la lacătul mecanic.

6.5. Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior, ușa biroului se încuie cu lacătul.

6.6. Înainte de acordarea accesului fizic la sistemul de evidență contabilă, se verifică competenţele de acces.

6.7. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

6.8. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidență contabilă, fiind integru din punct de vedere fizic.

6.9. Zilnic, se inspectează perimetrul de securitate al clădirii și al biroului, unde este amplasat sistemul de evidență contabilă, din punct de vedere fizic.

6.10. Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.

6.11. Uşile şi ferestrele sînt încuiate în cazul în care în încăpere lipsesc angajații autorizați de administrarea sistemului.

6.12. Amplasarea sistemului de evidență contabilă răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

6.13. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidență contabilă, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele de evidență contabilă, inclusiv posibilitatea deconectării oricărui component TI.

6.14. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidență contabilă, sînt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sînt separate de cele comunicaţionale.

6.15. Securitatea antiincendiară a sistemului de evidență contabilă: biroul unde este amplasat sistemul de evidență contabilă este dotat cu echipament antiincendiar și corespunde cerințelor și normelor antiincendiare în vigoare.

6.16. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemului de evidență contabilă. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

VII. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENȚĂ CONTABILĂ

7.1. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din sistemele de evidenţă contabilă şi a proceselor executate în numele acestor utilizatori.

7.2. Toţi utilizatorii (inclusiv personalul care asigură mentenanţa tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

7.3. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. Utilizarea parolelor în procesul asigurării securităţii informaţionale: pe lîngă cerinţele de păstrare a confidenţialităţii parolelor, este interzisă înscrierea acestora pe suport de hîrtie, cu excepţia cazului de asigurare a securităţii păstrării acesteia (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

7.4. Se efectuează modificarea parolelor de fiecare dată cînd sînt depistaţi indicii unei eventuale compromiteri a sistemului sau parolei.

7.5. Întru asigurarea posibilităţii de stabilire a responsabilităţii fiecărui utilizator, sînt folosite identificatori şi parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. După trei tentative greşite de autentificare, accesul este blocat, în mod automatizat.

7.6. Se asigură, pentru o perioadă de 1 */un/* an, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor şi prevenirea folosirii repetate a acestora.

7.7. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, şi, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum şi în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizaţii de acces primite în scopul comiterii unei fapte prejudiciabile, absenţă a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare şi autentificare se revocă sau se suspendă.

7.8. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidenţă contabilă, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidenţă contabilă, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 */una/* lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informaţiile din sistemul de evidenţă contabilă. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

7.9. În scopul depistării şi evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieşte cu regularitate, şi după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul de evidenţă contabilă.

7.10. Folosirea tehnologiilor fără fir, echipamentelor portative şi mobile se autorizează de persoanele responsabile.

7.11. Se impun limite în privinţa persoanelor care au dreptul:
a) să vizualizeze informaţiile stocate în sistemul de evidenţă contabilă;
b) să copieze, să descarce, să şteargă sau să modifice orice informaţie stocată.

7.12. Toţi angajaţii cu drepturi de acces beneficiază de o instruire iniţială în domeniul protecţiei datelor cu caracter personal.

7.13. Orice activitate de dezvăluire a datelor cu caracter personal către terţi este documentată şi supusă unei analize riguroase în prealabil privind scopul şi temeiul legal a intenţiilor de dezvăluire a unui anumit volum de date cu caracter personal.

7.14. Orice încălcare a securităţii în ceea ce priveşte sistemul de evidenţă contabilă este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cît de urgent posibil.

7.15. Înainte de acordarea accesului în sistem, utilizatorii sînt informaţi despre faptul că folosirea sistemului de evidenţă contabilă este controlată şi că folosirea neautorizată a acestora este sancţionată în conformitate cu legislaţia civilă, contravenţională şi penală.

VIII. AUDITUL SECURITĂŢII ÎN SISTEMELE DE EVIDENŢĂ CONTABILĂ

8.1. Se organizează generarea înregistrărilor de audit a securităţii în sistemul de evidenţă contabilă pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

8.2. Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:
a) data şi timpul tentativei intrării/ieşirii;
b) ID-ul utilizatorului;
c) rezultatul tentativei de intrare/ieşire – pozitivă sau negativă.

8.3. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării informaţiilor din sistemele de evidenţă contabilă, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:
a) data şi timpul tentativei de pornire;
b) denumirea/identificatorul programului aplicativ sau al procesului;
c) ID-ul utilizatorului;
d) rezultatul tentativei de pornire – pozitivă sau negativă.

8.4. Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării informaţiilor din sistemul de evidenţă contabilă, conform următorilor parametri:
a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau a procesului;
c) ID-ul utilizatorului;
d) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);
e) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);
f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) – pozitivă sau negativă.

8.5. Se efectuează înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:
a) data şi timpul modificării competenţelor;
b) ID-ul administratorului care a efectuat modificările;

c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

8.6. Se efectuează înregistrarea ieşirii din sistemul de evidenţă contabilă, înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:
a) data şi timpul eliberării;
b) denumirea informaţiei şi căile de acces la aceasta;
c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);
d) ID-ul utilizatorului care a solicitat informaţia;
e) volumul documentului eliberat (numărul paginilor, filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

8.7. Cazurile de deranjament al auditului securităţii în sistemul de evidenţă contabilă sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoștința persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

8.8. Rezultatele auditului securităţii în sistemul de evidenţă contabilă (operaţiunile de prelucrare a informaţiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidenţialităţii şi integrităţii acestora.

8.9. Durata minimă a stocării rezultatelor auditului securităţii în sistemul de evidenţă contabilă constituie 2 */doi/* ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

IX. ASIGURAREA INTEGRITĂŢII INFORMAŢIILOR DIN SISTEMUL DE EVIDENŢĂ CONTABILĂ

9.1. Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informaţiilor din sistemul de evidenţă contabilă, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestora, protecţia contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

9.2. Se utilizează tehnologii şi mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor şi constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informaţiilor din sistemul de evidenţă contabilă.

9.3. Se asigură testarea funcţionării corecte a componentelor de securitate a sistemului de evidenţă contabilă (automat – la pornirea sistemului, şi după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

9.4. Copiile de siguranţă: reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către operator intervalul de timp în care se execută copiile de siguranţă a informaţiilor din sistemul de evidenţă contabilă şi soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei indicate. Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ CONTABILĂ

10.1. Persoanele care asigură exploatarea sistemului de evidență contabilă trec, minimum o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

10.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidență contabilă.

10.3. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informațiilor din sistemul de evidență contabilă poartă răspundere civilă, contravenţională și penală.

XI. DISPOZIȚII FINALE

11.1. Prezentul Regulament este revizuit şi ulterior aprobat de către conducerea USEFS periodic, însă cel puțin o dată în an, precum și la necesitate.

11.2. Prezentul Regulament se completează cu prevederile legislației în vigoare.

11.3. Regulamentul este adus la cunoştinţa angajaților contra semnăturii.

11.4. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.